Mining Pools (*& Pool Hopping*)

- ★ Popular Mining Pool -Slush Pool using AWS Cloud Mining
- ★ Pool Hopping Attacks
- ★ How Slush Pool combats pool hopping
- ★ Slush Pool's Payout Scheme
- ★ Is Slush Pool still vulnerable?

Elsa Velazquez, MEd
Josh Nguyen

What are mining pools?

SOLO MINING

$$\frac{ht}{2^{32}D} = \frac{10^9\ \text{hash/s} \cdot 86400\ \text{s}}{2^{32} \cdot 1690906}$$

Poisson process: Block finding constant hashrate h= $\frac{h}{2^{32}D}$

Poisson distribution: number of blocks found= $\frac{ht}{2^{32}D}$,

In 24 hour time period:

- ➔ He finds it, he makes 50BTC
- ➔ On average, he therefore makes = 0.595 BTC
- ➔ Due to variance $\sqrt{\frac{2^{32}D}{ht}}$ the probability he will mine the right block is $1 - \exp(-\lambda) \approx 1.18\%$

The **total hashrate** of the Bitcoin system as of 5.11.2014

number of blocks in 1 year

$$\frac{283{,}494{,}086\ \text{GHash / s}}{1{,}700\ \text{GHash / s}} \approx 166{,}761 = 3.17 \cdot \overbrace{(365 \cdot 24 \cdot 6)}$$

The **hashrate of the Achilles Labs AM-1700 miner** (1095 USD)

The user has to wait on average over **3 years** to mine a block
(even if the difficulty does not increase!)

-Mining Pools and Attacks Stefan Dziembowski University of Warsaw Workshop on Bitcoin, June 2016

MINING POOLS

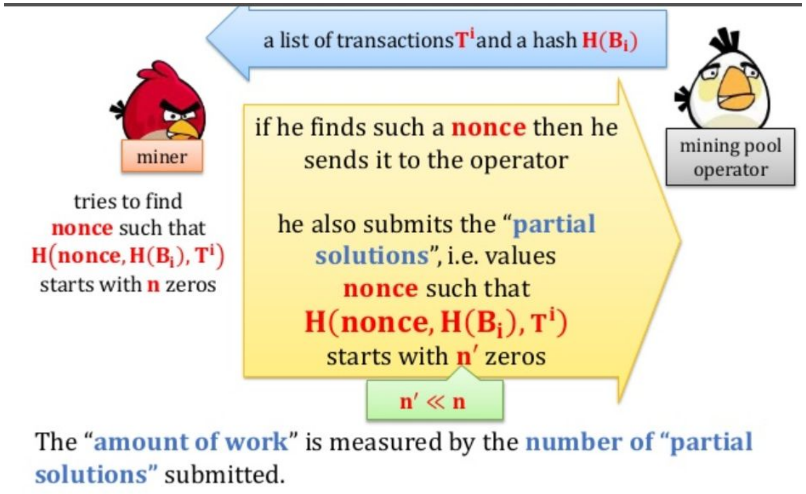
Poisson process: Block finding constant hashrate h = qH= $q^2\frac{HtB^2}{2^{32}D} = q\frac{htB^2}{2^{32}D}$

The reward is exactly the same, but the variance is far reduced: $q\frac{htB^2}{2^{32}D}$

The payout consider the pool operator’s fee: $\frac{(1-f)htB}{2^{32}D}$

The best payout: the smaller the miner and the bigger the pool (though this can change depending on the rewards system used).

What is the math behind mining pools?



a list of transactions $\mathbf{T^i}$ and a hash $\mathbf{H(B_i)}$

miner

tries to find **nonce** such that $\mathbf{H(nonce, H(B_i), T^i)}$ starts with **n** zeros

mining pool operator

if he finds such a **nonce** then he sends it to the operator

he also submits the "**partial solutions**", i.e. values **nonce** such that $\mathbf{H(nonce, H(B_i), T^i)}$ starts with $\mathbf{n'}$ zeros

$\mathbf{n' \ll n}$

The "**amount of work**" is measured by the **number of "partial solutions"** submitted.

Proportional method is implemented

Miners will perform hashs until a certain amount of leading zeros exist to fulfill the goal of n zeros. When miners find a partial solution, where n' leading zeros exist in the ending hash they may submit their work for partial solution towards the required n amount of zeros. Noting that n' is less than n for a partial solution. The partial solutions are then used to determine the ratio of payout once the block's reward has been issued and accpeted by the mining pool operator.

In this system, payments are calculated based on a division to rounds, where a round is the time between one block found by the pool to the next. When a block is found and the pool receives a reward of B, the operator keeps a fee of fB, and (1 − f)B are distributed among the miners,. If a miner submitted n shares in this round, and the total number of shares submitted to the pool during this round is N, then his payout for this round will be (n/N)*(1 − f)B.

Are all mining pools the same?

NO!!
There are many types:

Simple methods:
-Proportional
-Pay-per-share (PPS)

Score-based methods
-Slush's method
Geometric Method
Pay-per-last-N-shares (PPLNS)

Attempts for risk-free pay-per-share
-Maximum pay-per-share (MPPS)
-Shared maximum pay-per-share (SMPPS)
-Equalized SMPPS (ESMPPS)

Advanced methods
-Double geometric method
-General unit-based framework
-PPLNS variants

What is score-based method?

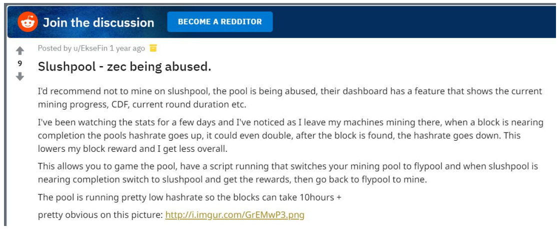
Slush's score-based method:

Attempts for risk-free pay-per-share
-Maximum pay-per-share (MPPS)
-Shared maximum pay-per-share (SMPPS)
-Equalized SMPPS (ESMPPS)

I'll do this one, too, since I did the research and posted the slide.

How is pool hopping detected?

First indication: Someone in the community notices when the block is nearing completion the hash rate goes up, then when the block is found the hashrate drops again.



Join the discussion BECOME A REDDITOR

Posted by u/EkseFin 1 year ago

9

Slushpool - zec being abused.

I'd recommend not to mine on slushpool, the pool is being abused, their dashboard has a feature that shows the current mining progress, CDF, current round duration etc.

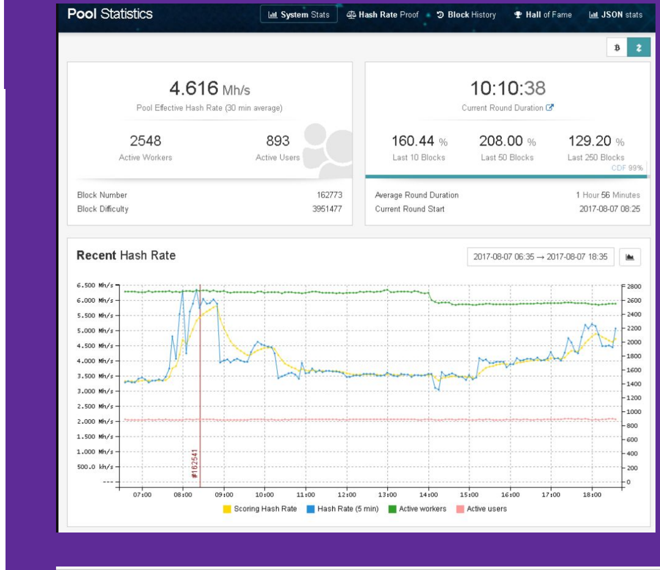
I've been watching the stats for a few days and I've noticed as I leave my machines mining there, when a block is nearing completion the pools hashrate goes up, it could even double, after the block is found, the hashrate goes down. This lowers my block reward and I get less overall.

This allows you to game the pool, have a script running that switches your mining pool to flypool and when slushpool is nearing completion switch to slushpool and get the rewards, then go back to flypool to mine.

The pool is running pretty low hashrate so the blocks can take 10hours +

pretty obvious on this picture: http://i.imgur.com/GrEMwP3.png

Second indication: Dramatic fluctuations in hash rates emerge around the event of a mined block.



Pool Statistics

4.616 Mh/s
Pool Effective Hash Rate (30 min average)

2548 Active Workers

893 Active Users

Block Number 162773

Block Dificulty 3951477

10:10:38
Current Round Duration

160.44 % Last 10 Blocks

208.00 % Last 50 Blocks

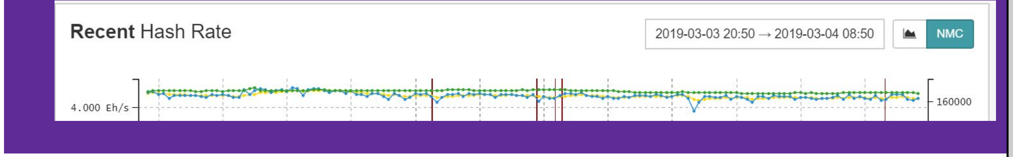
129.20 % Last 250 Blocks

CDF 99%

Average Round Duration 1 Hour 56 Minutes

Current Round Start 2017-08-07 08:25

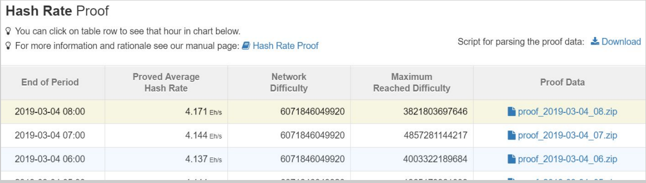
Recent Hash Rate 2017-08-07 06:35 → 2017-08-07 18:35



Recent Hash Rate 2019-03-03 20:50 → 2019-03-04 08:50

Final indication: The math adds up, but the payout doesn't.

1. Check proof of hash by examining the hash rate proof json file data.



Hash Rate Proof

You can click on table row to see that hour in chart below.

For more information and rationale see our manual page: Hash Rate Proof

Script for parsing the proof data: Download

End of Period	Proved Average Hash Rate	Network Difficulty	Maximum Reached Difficulty	Proof Data
2019-03-04 08:00	4.171 Eh/s	6071846049920	3821803697646	proof_2019-03-04_08.zip
2019-03-04 07:00	4.144 Eh/s	6071846049920	4857281144217	proof_2019-03-04_07.zip
2019-03-04 06:00	4.137 Eh/s	6071846049920	4003322189684	proof_2019-03-04_06.zip

2. Slush provides the complete block header + merkle branch + coinbase transaction for each collected submission and can prove the *pool operator* is honest and every miner is reporting accurately (called Share).

Proof that the hash rate is linearly dependent on the number of published block candidates:

3. ***However***, the miners that have remained faithfully committed see very few returns when a block is found because the payout is divided among all who sent in Shares. So, the pool hoppers make at least *SOME* money, collecting bags from every pool, which typically adds up to more than dedicated miners' gains. This is a threat to a pool because it could cause bankruptcy since it pays everyone who makes an effort, but miners have no reason to remain loyal to this pool with so many miners, and can choose to report mined blocks to smaller pools so they maximize on payout, leaving other Slush miners in the cold..

How are pool hoppers handled?

Incentive based payout methods are predefined to a pool to discourage pool hoppers. If interested there exist programs to help facilitate pool hopping around, for example:
https://bitcointalk.org/?topic=26866

Which mining pools are safest from pool hoppers?

PPS- No losses due to pool-hopping, which is ineffective against this method
However, this is the riskiest reward system for the pool operator- it could go bankrupt

This is a predetermined payment method with a flat payout method on each share solved. Takes out the variance of trying to mine the block and places all the variance on the pool operator. If things go well in a short round, the flat payment is good as where the operator gains the entire block reward but only has to give payment for less than the average number of shares – but can lose substantially on long rounds. In the long-run it should balance out to the statistical mean.

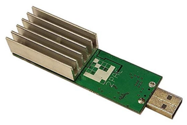
- No losses due to pool-hopping, which is ineffective against this method.

How do you join a mining pool?

★ Step 1- Research.

Ex: Running 10 of these is still at the very bottom of Bircoin mining and not worth it at all, takes almost 6 months to get a .001 payout into your walletThis is for suckers to loose money just trying it out

https://www.amazon.com/ask/questions/Tx2C45ML21ELPLW/1/ref=ask_al_cl_al_hza?expandComments=Mx12EJUTK5LSYDW



Rev 2 GekkoScience 2-Pac Compac USB Stick Bitcoin Miner 15gh/s+ (BM1384x2)

by GEKKOSCIENCE

★★★☆☆ 68 customer reviews

.

Hardware costs:

Minimum cost to make more than MAX ~$1/year (*maybe*) is $1400.

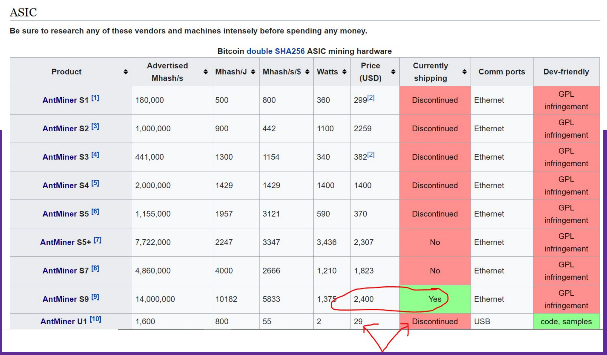
Using Low Cost Hardware:

GekkoScience Compac USB Stick Bitcoin Miner: > $1/ yr!

Avalon Nano 3: almost $1/yr.

Bitmain Antrouter R1 Wifi Solo Bitcoin Miner: a little over $1/ yr

https://www.bitcoinmining.com/usb-bitcoin-miners-bitcoin-mining/



ASIC

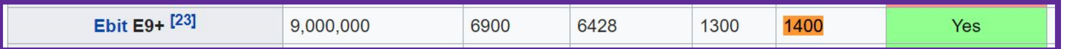
Be sure to research any of these vendors and machines intensely before spending any money.

Bitcoin double SHA256 ASIC mining hardware

Product	Advertised Mhash/s	Mhash/J	Mhash/s/$	Watts	Price (USD)	Currently shipping	Comm ports	Dev-friendly
AntMiner S1 [1]	180,000	500	800	360	299[2]	Discontinued	Ethernet	GPL infringement
AntMiner S2 [3]	1,000,000	900	442	1100	2259	Discontinued	Ethernet	GPL infringement
AntMiner S3 [4]	441,000	1300	1154	340	382[2]	Discontinued	Ethernet	GPL infringement
AntMiner S4 [5]	2,000,000	1429	1429	1400	1400	Discontinued	Ethernet	GPL infringement
AntMiner S5 [6]	1,155,000	1957	3121	590	370	Discontinued	Ethernet	GPL infringement
AntMiner S5+ [7]	7,722,000	2247	3347	3,436	2,307	No	Ethernet	GPL infringement
AntMiner S7 [8]	4,860,000	4000	2666	1,210	1,823	No	Ethernet	GPL infringement
AntMiner S9 [9]	14,000,000	10182	5833	1,375	2,400	Yes	Ethernet	GPL infringement
AntMiner U1 [10]	1,600	800	55	2	29	Discontinued	USB	code, samples

https://en.bitcoin.it/wiki/Mining_hardware_comparison

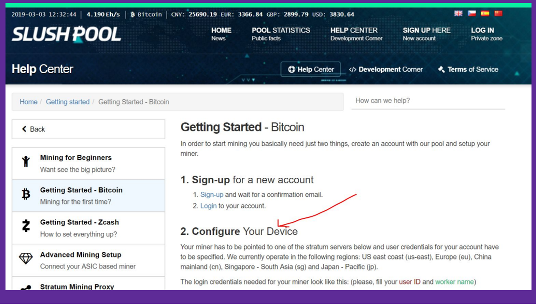
Using Least Cost Higher Performance Hardware:



Ebit E9+ [23]	9,000,000	6900	6428	1300	1400	Yes

Using Other Hardware:

Don't bother.



2019-03-03 12:32:44 | 4.190 Eh/s | Bitcoin | CNY: 25690.19 EUR: 3366.84 GBP: 2899.79 USD: 3830.64
SLUSH POOL
HOME News
POOL STATISTICS Public facts
HELP CENTER Development Corner
SIGN UP HERE New account
LOG IN Private zone
Help Center
Help Center
Development Corner
Terms of Service
Home / Getting started / Getting Started - Bitcoin
How can we help?
Back
Mining for Beginners Want see the big picture?
Getting Started - Bitcoin Mining for the first time?
Getting Started - Zcash How to set everything up?
Advanced Mining Setup Connect your ASIC based miner
Stratum Mining Proxy

Getting Started - Bitcoin

In order to start mining you basically need just two things, create an account with our pool and setup your miner.

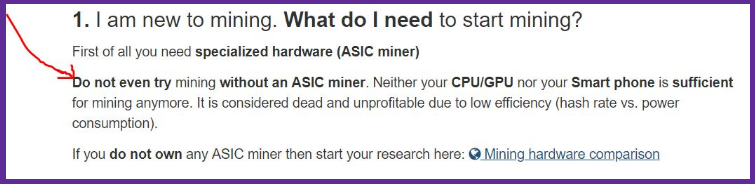
1. Sign-up for a new account

1. Sign-up and wait for a confirmation email.
2. Login to your account.

2. Configure Your Device

Your miner has to be pointed to one of the stratum servers below and user credentials for your account have to be specified. We currently operate in the following regions: US east coast (us-east), Europe (eu), China mainland (cn), Singapore - South Asia (sg) and Japan - Pacific (jp).

The login credentials needed for your miner look like this: (please, fill your user ID and worker name)



1. I am new to mining. **What do I need** to start mining?

First of all you need **specialized hardware (ASIC miner)**

Do not even try mining **without an ASIC miner**. Neither your **CPU/GPU** nor your **Smart phone** is **sufficient** for mining anymore. It is considered dead and unprofitable due to low efficiency (hash rate vs. power consumption).

If you **do not own** any ASIC miner then start your research here: Mining hardware comparison

How do you join a mining pool?

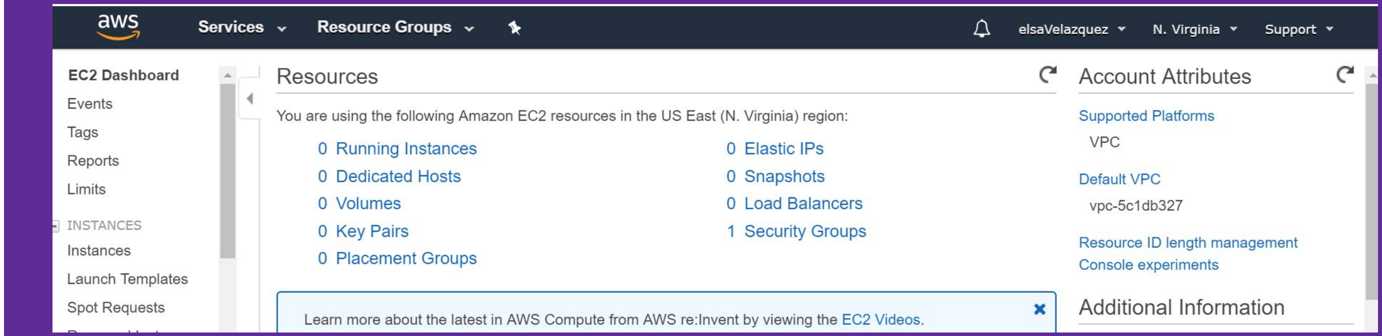
★ Step 2- Pick a method.

Pool Mining on the AWS Cloud:

AWS POOL https://medium.com/@codeAMT/how-to-mine-bitcoins-using-an-aws-ec2-instance-7604128c2c8f

Why AWS? Farms are "strategically located in countries with low-cost energy surplus and tax policies that can supply clean energy for our crypto mining production." https://bitcoinexchangeguide.com/aws-mining/

Also, cloud mining is an alternative to investing in hardware.



Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) region:

0 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
0 Volumes	0 Load Balancers
0 Key Pairs	1 Security Groups
0 Placement Groups	

Learn more about the latest in AWS Compute from AWS re:Invent by viewing the EC2 Videos.

Account Attributes

Supported Platforms
VPC

Default VPC
vpc-5c1db327

Resource ID length management
Console experiments

Additional Information

elve5895@colorado.edu

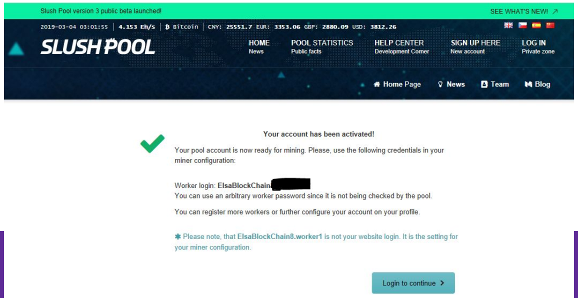
How do you join a mining pool?

★ Step 3- Pick a mining pool.

Slush Pool Mining

AWS POOL https://medium.com/@codeAMT/how-to-mine-bitcoins-using-an-aws-ec2-instance-7604128c2c8f

Why Slush Pool? As noted by outspoken miners, their GUI is by far the best, and they have credibility as the first mining pool ever established.



2019-03-04 03:01:55 | 4.153 Eh/s | ฿ Bitcoin | CNY: 25551.7 EUR: 3353.06 GBP: 2880.09 USD: 3812.26

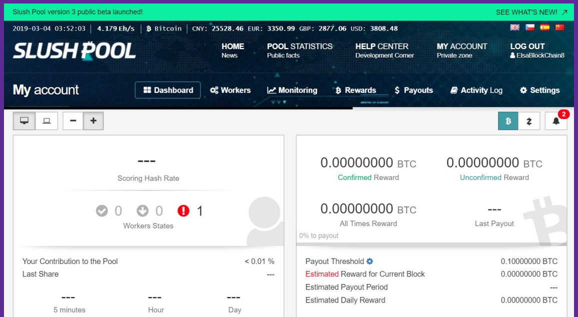
Your account has been activated!

Your pool account is now ready for mining. Please, use the following credentials in your miner configuration:

Worker login: **ElsaBlockChain[redacted]**
You can use an arbitrary worker password since it is not being checked by the pool.

You can register more workers or further configure your account on your profile.

✱ Please note, that **ElsaBlockChain8.worker1** is not your website login. It is the setting for your miner configuration.



2019-03-04 03:52:03 | 4.179 Eh/s | ฿ Bitcoin | CNY: 25528.46 EUR: 3350.99 GBP: 2877.06 USD: 3808.48

Scoring Hash Rate

✓ 0 ↓ 0 ! 1
Workers States

Your Contribution to the Pool < 0.01 %
Last Share ---

--- 5 minutes | --- Hour | --- Day

0.00000000 BTC Confirmed Reward
0.00000000 BTC Unconfirmed Reward
0.00000000 BTC All Times Reward
--- Last Payout
0% to payout

Payout Threshold 0.10000000 BTC
Estimated Reward for Current Block 0.00000000 BTC
Estimated Payout Period ---
Estimated Daily Reward 0.00000000 BTC

How do you join a mining pool?

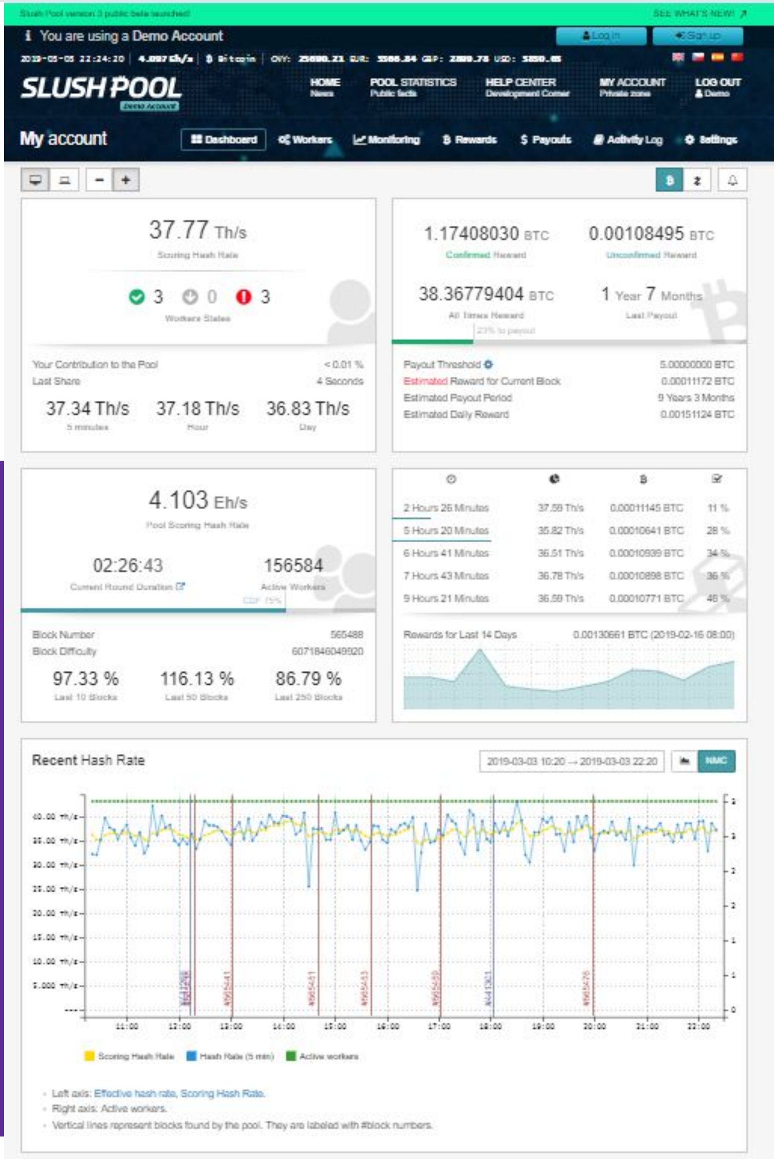
The Slush Pool Interface

JOSH

https://slushpool.com/dashboard/?c=btc

can you be familiarized with
the whole demo interface?

Feel free to do stuff with your slides,
I'm just trying to create some kind of outline



ℹ You are using a Demo Account

2019-03-03 22:24:20 | 4.097 Eh/s | ₿ Bitcoin | CNY: 25880.21 EUR: 3386.84 GBP: 2889.78 USD: 3850.65

My account

37.77 Th/s
Scoring Hash Rate

✓ 3 0 ! 3
Workers States

Your Contribution to the Pool	< 0.01 %
Last Share	4 Seconds

37.34 Th/s	37.18 Th/s	36.83 Th/s
5 minutes	Hour	Day

1.17408030 BTC
Confirmed Reward

0.00108495 BTC
Unconfirmed Reward

38.36779404 BTC
All Times Reward

1 Year 7 Months
Last Payout

23% to payout

Payout Threshold	5.00000000 BTC
Estimated Reward for Current Block	0.00011172 BTC
Estimated Payout Period	9 Years 3 Months
Estimated Daily Reward	0.00151124 BTC

4.103 Eh/s
Pool Scoring Hash Rate

02:26:43
Current Round Duration

156584
Active Workers

CDF 75%

Block Number	565488
Block Difficulty	6071846049920

97.33 %	116.13 %	86.79 %
Last 10 Blocks	Last 50 Blocks	Last 250 Blocks

⏱	◔	₿	☑
2 Hours 26 Minutes	37.58 Th/s	0.00011145 BTC	11 %
5 Hours 20 Minutes	35.82 Th/s	0.00010641 BTC	28 %
6 Hours 41 Minutes	36.51 Th/s	0.00010939 BTC	34 %
7 Hours 43 Minutes	36.78 Th/s	0.00010898 BTC	36 %
9 Hours 21 Minutes	36.58 Th/s	0.00010771 BTC	46 %

Rewards for Last 14 Days 0.00130661 BTC (2019-02-16 08:00)

Recent Hash Rate

2019-03-03 10:20 → 2019-03-03 22:20

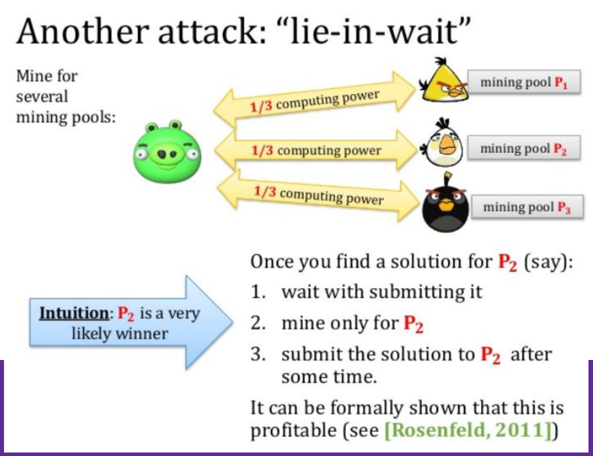
- Left axis: Effective hash rate, Scoring Hash Rate.
- Right axis: Active workers.
- Vertical lines represent blocks found by the pool. They are labeled with #block numbers.

What protocols keep pools safe from pool hoppers?

- SLUSH protocols- it does not have protocols against pool hopping
- Preventing pool-hopping is simple: When creating a pool, simply choose an algorithm for funds distribution that has been proven immune or even hostile to hopping - i.e. anything but proportional. When choosing a pool to mine in, one should similarly choose a pool which has chosen a fair payment schema.

What are other common attacks on mining pools?

Block withholding



Another attack: “lie-in-wait”

Mine for several mining pools:

1/3 computing power

1/3 computing power

1/3 computing power

mining pool P_1

mining pool P_2

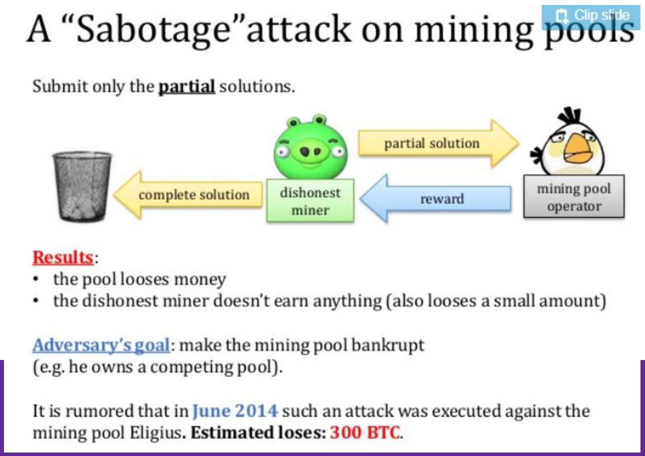
mining pool P_3

Intuition: P_2 is a very likely winner

Once you find a solution for P_2 (say):

1. wait with submitting it
2. mine only for P_2
3. submit the solution to P_2 after some time.

It can be formally shown that this is profitable (see [Rosenfeld, 2011])



A “Sabotage”attack on mining pools

Submit only the **partial** solutions.

complete solution

dishonest miner

partial solution

reward

mining pool operator

Results:

- the pool looses money
- the dishonest miner doesn’t earn anything (also looses a small amount)

Adversary's goal: make the mining pool bankrupt (e.g. he owns a competing pool).

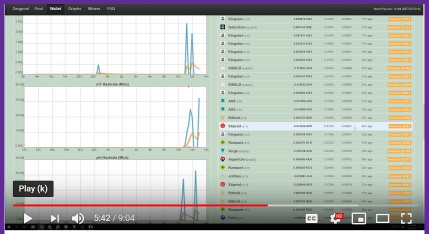
It is rumored that in **June 2014** such an attack was executed against the mining pool Eligius. **Estimated loses: 300 BTC**.

“The well-known sabotage - not submitting blocks at all to cause financial harm to the pool or its participants.
The lesser-known lie-in-wait - delay submitting of a block, and use knowledge of the imminent block for extra profit.”
Meni Rosenfeld

Do all mining pools make money?

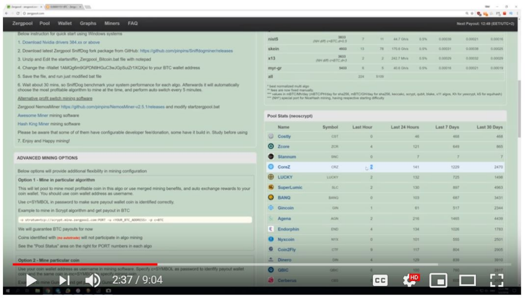
NO!! And, according to many reviews, it is mostly dependent on luck and the rate of pool hopping.

- ★ Miner A checks his earnings via his wallet, and demonstrates payout is all luck because there is no trend. https://www.youtube.com/watch?v=WkHMCmoD_go



How do mining pools calculate your profit, Shares, Difficulty and Luck Explained

- ★ Miner A shows that it’s not possible to make payout comparisons depending on coins because it’s apples to oranges.



How do mining pools calculate your profit, Shares, Difficulty and Luck Explained

- ★ Miner B explains he made almost nothing from Slush Pool because they do not guard against Pool Hopping, so he fled to Fly Pool.
- ★ Miner B claims his mining payout has eclipsed his day-job earnings, however he also states he accrued massive debt and has electricity bills at $1k/month, and so did not clearly distinguish profit from income in running his own elaborate mining farm.

So, is mining profitable?

Most sources say no.

- Is Amazon cloud mining Illegal? "No, but you'll spend more than you'll get in BTC.", "Not illegal on any (virtual) computer. Unlikely to be profitable though." https://www.reddit.com/r/aws/comments/7559s1/is_it_illegal_to_cryptocurrency_mining_on_aws/
- "...you will likely see that *some* cloud mining services will be profitable for a few months, but, as the difficulty level of bitcoin increases, you would probably start to make a loss in four to six months and beyond." - https://www.coindesk.com/information/cloud-mining-bitcoin-guide
-

What is the future of mining pools?

Quantum Computing and Pool Hopping

Quantum Computers Are the Most Powerful Tech Threat to Cryptocurrency. - Peter Keay, March 14 2018

- ★ Google claims to have advanced beyond [49-qubit quantum computer in July of 2017 to] Bristlecone, a 72-qubit computerwhich Google is working to bring down to reasonable error rates.
- ★
- ★ ***Definition*: 51% attack,** a commonly discussed attack on a cryptocurrency where a malicious actor or pool of actors controls enough of the mining power on the cryptocurrency's network to control the network to some degree. Despite the attack's name, the power required can be lower than 51%.
- ★ A quantum computer's power could possibly be used to dominate proof of work power on a network and execute a 51% attack. However, for several reasons, I see this as an improbable quantum attack on a cryptocurrency
- ★ https://blog.icoalert.com/quantum-computers-are-the-most-powerful-tech-threat-cryptocurrency-will-face
- ★ Hshare's Hcash is implementing BLISS signatures for quantum resistance. In fact, it is a version of BLISS that Hshare claims is "faster, hardened against side-channel attacks, power analysis and 51% attacks."

elve58

https://blog.icoalert.com/quantum-computers-are-the-most-powerful-tech-threat-cryptocurrency-will-face